CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method in a computer-based environment for preparing content to be deployed on a target wireless device, comprising:

   selecting the content from the group consisting of locally stored applications, remotely stored, trusted applications and remotely stored, untrusted applications;

   provisioning the content for the target device; wherein when the content is selected from the remotely stored, untrusted applications, the provisioning comprises intercepting the content and inspecting the content, wherein the inspecting comprises at least one of examining the content to detect malicious code, determining whether the content contains banned code, and determining whether the content contains designated API;

   verifying that the device supports execution of the content by comparing the device capabilities to the content requirements; and

   providing the verified and provisioned content to the target device.

2. (Original) The method of claim 1, further comprising causing the prepared content to downloaded to the target device over a wireless transmission medium.
3. (Original) The method of claim 2 wherein the content is requested by a subscriber of a carrier to the computer-based environment over a wireless transmission medium.
4. (Original) The method of claim 1 wherein the provisioning comprises at least one of: inspecting the content; optimizing the content; and instrumenting the content.
5. (Currently Amended) The method of claim [[4]] 1 wherein the provisioning comprises inspecting the content, wherein inspecting the content comprises an operation selected from the group consisting of deconstructing a stucture of the content, checking for malicious code, checking for banned code, determining the applicable application of filters, and checking a number of activated threads. ~~the inspecting further comprising at least one of: determining whether the content~~

PAGE 4/21 * RCVD AT 10/24/2005 1:27:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-06

~~contains malicious code; determining whether the content contains banned code; and determining whether the content contains designated API.~~

6. (Currently Amended) The method of claim 5 wherein the inspecting further comprises determining whether the application contains designated API, wherein the API is at least one of packages, classes, methods, and fields.
7. (Currently Amended) The method of claim [[4]] 5 wherein the ~~inspecting is performed using an application filter~~ determining the applicable application of filters comprises retrieving an application filter relevant for potential targets under examination, wherein the application filter detects one of package and method names, package and method classes, package and method fields, API suspected to have intrusive behavior, API suspected to have malicious behavior and API that are unauthorized for use.
8. (Currently Amended) The method of claim [[7]] 4 wherein the provisioning comprises inspecting the content, wherein the inspecting is performed using an application filter, wherein the application filter specifies a list of criteria to be filtered and a target.
9. (Original) The method of claim 8 wherein the criteria is an API.
10. (Original) The method of claim 8 wherein that target is at least one of a specified client, device type, content identifier, and global definition.
11. (Currently Amended) The method of claim 4 [[,]] wherein the provisioning comprises optimizing the content, wherein the optimizing ~~further comprising~~ comprises at least one of: reducing the size of variable names; modifying instructions to more efficient instructions; mapping executable paths in code; and removing unused code.
12. (Currently Amended) The method of claim 4 [[,]] wherein the provisioning comprises ~~the~~ instrumenting the content, wherein the instrumenting ~~further comprising~~ comprises inserting code that implements at least one of a billing policy, a usage policy, a notification, and an automatic content update mechanism.
13. (Currently Amended) The method of claim [[4]] 1 wherein the verifying that the device supports execution of the content further comprises identifying a device,

PAGE 5/21 * RCVD AT 10/24/2005 1:27:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-06

accessing capabilities of the device from a device profile, accessing device requirements of the content, and determining whether resources required by the content are available according to the device profile ~~wherein the instrumenting is accomplished at a byte-code level of content examination~~.

14. (Currently Amended) The method of claim [[1]] 13 wherein the device profile contains information relevant to the capabilities of the device, wherein the information relevant to the capabilities of the device are selected from the group consisting of memory capacity, processor type, processing speed, and maximum size of a downloadable application ~~wherein the provisioning provides code to support billing policies~~.
15. (Currently Amended) The method of claim [[14,]] 12 wherein the billing ~~policies~~ policy ~~further comprising~~ comprises at least one of subscription based billing, trial use, download based billing, transmission based billing, and prepaid billing.
16. (Currently Amended) The method of claim [[14]] 15 wherein the billing ~~policies are~~ policy is provided by a wireless carrier infrastructure.
17. (Currently Amended) The method of claim 1 wherein the content is provisioned for a requestor ~~requester~~, and the verifying further comprising at least one of: comparing the API used by the content to the API supported by the target device[[;]] and determining whether the requestor is authorized to use the content; ~~and determining whether the content is banned~~.
18. (Currently Amended) The method of claim 17 wherein determining whether the requestor is authorized determines whether the ~~requester~~ requestor has sufficient funds in a prepaid billing account to use the content.
19. (Original) The method of claim 1 wherein the verification is accomplished using profile management.
20. (Original) The method of claim 19 wherein the profile management defines profiles for at least one of a subscriber, device type, and content.
21. (Original) The method of claim 1 wherein the content is Java-based.
22. (Original) The method of claim 1 wherein the environment is integrated with a wireless carrier infrastructure.

PAGE 6/21 * RCVD AT 10/24/2005 1:27:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-05

23. (Original) The method of claim 1 wherein the content preparation provides walled-garden provisioning.
24. (Original) The method of claim 1, the computer-based environment including a network, wherein the provisioning supports the designation of the content to be prepared through browsing to a location on the network.
25. (Original) The method of claim 1 wherein the network is the Internet.
26. (Currently Amended) The method of claim 1 wherein the preparation process takes into account preferences of a ~~requester~~ requestor of the content.
27. (Original) The method of claim 1 wherein attributes that control the provisioning are specified through website administration.
28. (Currently Amended) The method of claim 1 ~~wherein attributes that control the verification are specified through website administration~~ wherein the provisioning comprises preparing an initial list of available applications.
29. (Original) The method of claim 1 wherein the content contains at least one of text, graphics, audio, and video.
30. (Currently Amended) A network-based transmission ~~medium~~ system comprising: ~~containing~~
a deployment manager configured to retrieve an application from one of the group consisting of locally stored data repositories, trusted, third party application providers, and untrusted, third party hosts; and
an inspector, wherein when the application is retrieved from an untrusted, third party host, the inspector examines the application by a method selected from the group consisting of examining the application to detect malicious code, performing a class analysis of the application to verify that classes in the application conform to desired standards, applying application filters to the application ~~content that has been provisioned and verified specifically for a target wireless device~~.
31. (Currently Amended) The transmission ~~medium~~ system of claim 30 wherein the ~~content~~ application is transmitted to the target wireless device.
32. (Currently Amended) The transmission ~~medium~~ system of claim 30, ~~wherein the provisioned content~~ further comprising at least one of an optimizer and an

PAGE 7/21 * RCVD AT 10/24/2005 1:27:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-06

instrumentation analyzer, wherein the optimizer is configured to reduce a code size of the application when possible, and wherein the instrumentation analyzer is configured to modify code in the application according to specified policies ~~has been at least one of inspected, optimized, and instrumented~~.

33. (Currently Amended) The transmission ~~medium~~ system of claim [[32]] 30 wherein ~~inspected content has been inspected to determine that it does not contain specified code, API, or other criteria~~ the desired standards are selected from the group consisting of number of API calls, type of API call, and frequency of API calls.

34. (Canceled) ~~The transmission medium of claim 32 wherein the inspected content has been inspecting using dynamically specifiable application filters~~.

35. (Currently Amended) The transmission ~~medium~~ system of claim [[34]] 30 wherein the application filters comprise dynamically specifiable filters, wherein the dynamically specifiable filters specify a list of criteria to be filtered and a target.

36. (Currently Amended) The transmission ~~medium~~ system of claim 32 wherein the instrumentation analyzer inserts code into the application configured ~~instrumented content contains code~~ to implement at least one of a billing policy, usage policy, notification, and automated content update mechanism.

37. (Canceled) ~~The transmission medium of claim 32 wherein the instrumented content has been instrumented at the byte-code level~~.

38. (Canceled) ~~The transmission medium of claim 30 wherein the provisioned content contains code to automatically implement a billing policy for the content~~.

39. (Currently Amended) The transmission ~~medium~~ system of claim 30, further comprising a provisioning manager configured to verify whether a target device supports execution of the application by a method selected from the group consisting of ~~wherein the content has been verified by~~ determining at least one of a user of the target device is authorized to receive the ~~content~~ application, determining whether the target device supports ~~the~~ an API used by the application ~~content~~, and determining whether the ~~content~~ application has not been banned.

PAGE 8/21 * RCVD AT 10/24/2005 1:27:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-06

40. (Currently Amended) The transmission ~~medium~~ system of claim 30, further comprising a provisioning manager configured to verify whether a device supports execution of the application by identifying the device, accessing capabilities of the device from a device profile, accessing device requirements of the application, and determining whether resources required by the application are available according to the device profile ~~wherein the content has been verified by comparing aspects of the content to stored profiles~~.

41. (Currently Amended) The transmission ~~medium~~ system of claim 30 wherein the ~~network~~ system is connected to a wireless carrier infrastructure.

42. (Currently Amended) The transmission ~~medium~~ system of claim 30 wherein the ~~content~~ application is Java-based.

43. (Currently Amended) The transmission ~~medium~~ system of claim 30 wherein the ~~network~~ deployment manager is coupled to the Internet.

44. (Currently Amended) The transmission ~~medium~~ system of claim 30 wherein the ~~content~~ application contains at least one of text, graphics, audio, and video.

45. (Currently Amended) A ~~computer-readable memory medium~~ mobile applications system operable in conjunction with a computer processor, the mobile applications system ~~containing instructions~~ comprising a system application operable to ~~for~~ control~~ling~~ a computer processor to prepare content for deployment on a target device, such that the computer processor fetches a retrieved application from one of the group consisting of locally stored data repositories, trusted, third party application providers, and untrusted, third party hosts;

examines the retrieved application by a method selected from the group consisting of examining the retrieved application to detect malicious code, performing a class analysis of the retrieved application to verify that classes in the retrieved application conform to desired standards, and applying application filters to the retrieved application; ~~content that has been provisioned and verified specifically for a target wireless device by: provisioning the content for the target device; and verifying~~ verifies that the target device supports execution of the ~~provisioned~~

PAGE 9/21 * RCVD AT 10/24/2005 1:27:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-06

~~content~~ retrieved application without executing the ~~provisioned content~~ retrieved application on the device.

46. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 45 wherein the target device is a wireless device.

47. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 45 [[,]] wherein the system application causes ~~wherein the instructions further comprise causing~~ the ~~prepared content~~ retrieved application to be downloaded to the target device over a wireless transmission medium.

48. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 45 [[,]] wherein the retrieved application is ~~the provisioning further comprising~~ at least one of: ~~inspecting the content; optimizing the content;~~ optimized and instrumented ~~instrumenting the content~~.

49. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 48 [[,]] wherein the system application causes the computer processor to ~~the inspecting further comprising at least one of: determining~~ determine whether the ~~content~~ retrieved application contains an element selected from the group consisting of malicious code; ~~determining whether the content contains~~ banned code; and ~~determining whether the content contains~~ designated API.

50. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 48 wherein the system application causes the computer processor to apply ~~inspecting is performed using~~ an application filter to the retrieved application.

51. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 48 [[,]] wherein the system application causes the computer processor to ~~the instrumenting further comprising inserting~~ insert code that implements at least one of a billing policy, a usage policy, a notification, and an automatic content update mechanism.

52. (Canceled) ~~The computer-readable memory medium of claim 48 wherein the instrumenting is accomplished at a byte-code level of content examination~~.

PAGE 10/21 * RCVD AT 10/24/2005 1:27:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-08

53. (Canceled) ~~The computer-readable memory medium of claim 45 wherein the provisioning provides code to support billing policies~~.

54. (Canceled) ~~The computer-readable memory medium of claim 53, the billing policies further comprising at least one of subscription based billing, trial use, download based billing, transmission based billing, and prepaid billing~~.

55. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 45 wherein the system application causes the computer processor to ~~content is provisioned for a requester, and wherein the verification further comprises at least one of: comparing~~ compare ~~the~~ an API used by the ~~content~~ retrieved application to ~~the~~ an API supported by the target device; ~~determining~~ determine whether the requestor is authorized to use the content; and ~~determining~~ determine whether the content is banned.

56. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 55 wherein ~~determining authorization of~~ the requestor ~~determines whether~~ is authorized where the ~~requester~~ requestor has sufficient funds in a prepaid billing account to use the ~~content~~ retrieved program.

57. (Canceled) ~~The computer-readable memory medium of claim 45 wherein the verification is accomplished using profile management~~.

58. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 45 wherein the ~~content~~ retrieved application is Java-based.

59. (Canceled) ~~The computer-readable memory medium of claim 45 wherein the provisioning supports the designation of the content to be prepared through browsing to a location on a network~~.

60. (Currently Amended) The ~~computer-readable memory medium~~ mobile applications system of claim 45 wherein the content contains at least one of text, graphics, audio, and video.

61. (Currently Amended) A computer-based content deployment system for provisioning content for a target device, comprising:
a verification manager that verifies that the content is authorized and the target device supports resources needed by the content;

PAGE 11/21 * RCVD AT 10/24/2005 1:27:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-06

a deployment manager coupled to and operational with the verification manager, the deployment manager configured to retrieve the content from one of the group consisting of locally stored data repositories, trusted, third party application providers, and untrusted, third party hosts;

an inspector, coupled to and operational with the verification manager and deployment manager, wherein when the content is retrieved from an untrusted, third party host, the inspector examines the content by a method selected from the group consisting of examining the content to detect malicious code, performing a class analysis of the content to verify that classes in the content conform to desired standards, applying application filters to the content;

and a provisioning manager, operable with and coupled to the verification manager, the deployment manager and the inspector, that provisions the content according to the target device by at least one of inspecting the content, optimizing the content, and instrumenting the content.

62. (Original) The deployment system of claim 61 wherein the provisioning manager further comprises at least one of: subscriber verifier; device verifier; and application verifier.

63. (Original) The deployment system of claim 62 wherein the subscriber verifier determines whether a subscriber of a wireless carrier service is authorized to use the content.

64. (Original) The deployment system of claim 62 wherein the device verifier determines whether the target device supports an API required by the content.

65. (Original) The deployment system of claim 62 wherein the application verifier determines whether the content is banned.

66. (Original) The deployment system of claim 61 wherein the target device is a wireless device.

67. (Original) The deployment system of claim 61 wherein the deployment system is integrated with a wireless carrier computer system.

68. (Original) The deployment system of claim 61 wherein instrumenting the content provides support for at least one of a billing policy, a usage policy, a notification, and an automatic content update mechanism.

PAGE 12/21 * RCVD AT 10/24/2005 1:27:58 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-08

69. (Currently Amended) The deployment system of claim 61, further comprising: a billing manager, coupled to an operable with the provisioning manager, that provides support for provisioning the content according to a billing policy.
70. (Original) The deployment system of claim 69 wherein the billing policy is one of subscription base billing, trial use, download based billing, transmission based billing, and prepaid billing.
71. (Original) The deployment system of claim 61 wherein the designation of the content to be provisioned is determining by browsing to a location on a network.
72. (Original) The deployment system of claim 61 wherein the content is Java-based.
73. (Original) The deployment system of claim 61 wherein the content contains at least one of text, graphics, audio, and video.

PAGE 13/21 * RCVD AT 10/24/2005 1:27:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:404 880 9912 * DURATION (mm-ss):08-06